CHAOS 2010, 3rd Chaotic Modeling and Simulation International Conference, Chania, Crete, Greece, 1 - 4 June 2010

Modified Chaotic Shift Keying using Indirect Coupled Chaotic Synchronization for Secure Digital Communication

Rupak Kharel, Krishna Busawon, Z. Ghassemlooy

University of Northumbria, Newcastle Upon Tyne,United Kingdom
Email: rupak.kharel@unn.ac.uk

Abstract: In this paper, a modified chaotic shift keying method is proposed to transmit digital bits securely over a communication channel. The scheme is based upon encrypting the digital bits 0 and 1 into infinite levels by applying the keystream such that there is no recognisable pattern in the encoded transmitted signal. The encoded transmitting signal generated is shown to resist popular attack method therefore realizing a secure and trustworthy digital communication system.

Keywords: Chaotic synchronization, Chaotic shift keying, Secure Communication, Return Maps, Encryption, Chaotic simulation.

1. Introduction

For the last decade or so, the use of chaotic signals for transmitting messages securely over a channel have attracted a great deal of attention amongst researchers [1]. Chaotic signals have properties such as aperiodicity, sensitivity to initial conditions/parameter mismatches and have fundamentally broadband like nature. The main idea of using chaotic signal in secure communication is to bury the message spectrum/plaintext into the broad chaos spectrum; equivalent to burying inside the noise. At the receiver, chaotic synchronization is performed and the plain text message is revealed by performing some sort of inversion. Different methods are available in the literature which are Chaotic Masking, Chaotic Modulation, Chaotic Inclusion technique and Chaotic Shift Keying (CSK) [1]. Variations of these methods are also proposed but almost all of them fall on one or more of the above categories.

Chaotic masking is the first method proposed and is the simplest of all where the chaotic signal acts as a mask on which the message/plaintext is added to form the transmitted chaotic signal. In chaotic modulation, the message is used to modulate some parameter(s) of the chaotic system. In the so-called chaotic inclusion technique, the message is used to change the chaotic attractor directly at the phase space. The CSK method was proposed for transmitting binary signals and is fundamentally a special case of chaotic modulation. The transmitting bit either 0 or 1 determines the value of the parameter to be switched of the chaotic systems. At the receiver, chaotic synchronization is performed by setting parameter of the chaotic system equivalent to one of the bit value. By thresholding the synchronization error

at the receiver, the transmitted binary value can easily be determined.
Chaotic masking was shown to be insecure by various methods including Short's, return map analysis [1, 2]. The insecurity was shown for other methods, in particular, for CSK [2, 3], parametric modulation [2], and inclusion method [2]. Modification to these methods [4, 5] have also been proposed but to no avail [6, 7]. Other proposed methods based on the projective synchronization [8], phase synchronization [9], generalized synchronized were broken as well [10, 11]. Methods based on the time delay or the hyperchaos were also sought for increasing the security but they too were not entirely convincing (see eg. [12, 13]). Therefore, there is still a need to improve the existing methods if secure communication is to be realized using chaotic signals.
In this paper, we propose a methodology for improving the traditional CSK method by using the indirect coupling synchronization of the chaotic oscillators as developed in [14]. The main purpose of using indirect coupled synchronization is to generate synchronized keystream in the transmitter and receiver side. The binary signal to be transmitted will be modulated by an encrypted chaotic parameter using the keystream and encryption function into infinite levels between a given interval. This brings a considerable improvement on the traditional CSK method. In particular, we show that the proposed modified CSK method resists powerful decryption attacks such as return maps based attacks.
This paper is organized as follows. In Section 2, the modified CSK scheme for secure communication will be proposed. In Section 3, the implementation of the proposed technique using Lorenz and Chua's oscillator will be shown and simulation results to show successful message extraction will be presented. In Section 4, cryptanalysis of the proposed method using return map analysis will be discussed. Finally some concluding remarks will be made on Section 5.

2. Problem Statement

Consider a chaotic system with parameter β and output y described as follows:

$$\dot{x} = f(x, y, \beta)$$
$$y = h(x)$$

where $x \in R^n$ and $y \in R$. The function f and h are assumed to be smooth.
In CSK, the basic idea is to switch the parameter β of the chaotic system into two values depending on either 0 or 1 is to be transmitted, as follows:

$$\beta = \beta_m = \begin{cases} \beta_0 \text{ when } m = 0 \\ \beta_1 \text{ when } m = 1. \end{cases}$$

Upon receiving the modulated chaotic signal, the receiver is set with either of the parameters β_0 or β_1. Now, when the binary value m=0 is transmitted

(β_0 used in receiver), synchronization is achieved; otherwise, synchronization is not possible, which constitute the basis for recovering the transmitted bits. Generally, in practice, some specific pattern associated with the transmitted chaotic signal can be observed when different binary values are sent. This is mainly due to some sort of switching involved in the process. Recovering the bits for intruders can simply amount to a classification problem, which can easily be done by methods such as return maps as explained in [2] or artificial neural network as in [3]. Thus, although CSK provides possibly the best way to transmit binary message using chaotic signals, it is not at all secure. Variations of CSK method have been reported such as in [15] but were not entirely convincing as shown in [16]. Therefore, in this paper, an effort is made to remove or blur any sort of pattern in the transmitted chaotic signal due to the switching of binary values.

3. Proposed Modified CSK method

The proposed modified CSK method is illustrated in Figure 1.
We consider the following system to be used as transmitter

$$(\mathrm{T}):\begin{cases}\dot{x}=f(x,y_1,\beta_m)\\ y_1=g_1(x)\\ y_2=g_2(x)\end{cases}\quad \text{where } \beta_m=\begin{cases}\beta_0=\beta+e(0,k) \text{ if } m=0\\ \beta_1=\beta+e(\rho,k) \text{ if } m=1.\end{cases}$$

and $x\in R^n$ and $y\in R$. The function f, g_1 and g_2 are assumed to be smooth.

Here β_m is the parameter to be modulated and $e(.)$ is an encryption algorithm, ρ is a constant scalar and k is the keystream for performing encryption. The function $e(.)$ is chosen such that its values (or image), $e(\rho, k)$, falls within the interval $[-h, h]$ where h is an encryption parameter. Therefore, β_m will always be in the interval $[-h+\beta, h+\beta]$. With the proper choice of h, it can be ensured that β_m always falls within the range such that (T) remains chaotic. y_1 is the transmitted signal for synchronization to the receiver described by:

$$(\mathrm{R}):\begin{cases}\dot{\hat{x}}=f(\hat{x},y_1,\hat{\beta}_m)\\ y_2=g_2(\hat{x}),\end{cases}\text{ where } \hat{\beta}_m=\beta_0=\beta+e(0,\hat{k}).$$

Here also we have $-h+\beta \le \hat{\beta}_m \le h+\beta$. If synchronization is achieved, it can be concluded that 0 is transmitted otherwise 1 is transmitted. The keystreams k and $\hat{k}$ are generated using indirect coupled synchronization and the systems for generating them are defined as

$$(\mathrm{A}):\begin{cases}\dot{u}=p(u,y_2)\\ k=q(u)\end{cases}\text{ and }(\mathrm{B}):\begin{cases}\dot{\hat{u}}=p(\hat{u},\hat{y}_2)\\ \hat{k}=q(\hat{u}).\end{cases}$$

The systems defined by (A) and (B) are driven by y_2 and $\hat{y}_2$ respectively

such that the keystreams are synchronized. It should be noted that y_2 and $\hat{y}_2$ are not always equal since the parameter β_m in the transmitter and the receiver are varying. In the transmitter, it is changing according to both binary values but in the receiver, it is changing only due to the binary value 0. But synchronization is still achievable for the keystream generating oscillator as shown later in the simulation results.

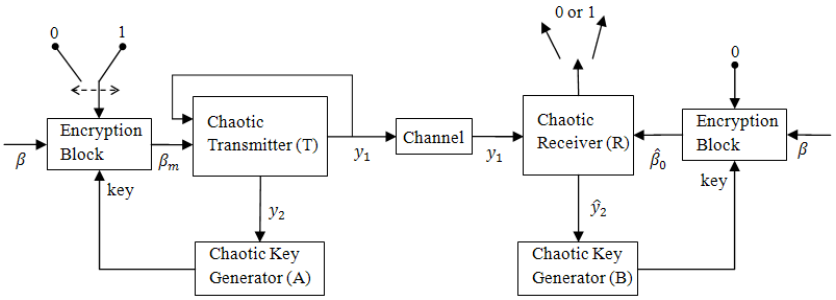

Figure 1. Modified CSK Method

3. Implementation using Lorenz and Chua's system

The proposed method is implemented using the Lorenz and Chua system. The Lorenz system acting as transmitter and receiver are given as

$$(\mathrm{T}):\begin{cases}\dot{u}=-\sigma y_1+\sigma v\\ \dot{v}=-20y_1w+ry_1-v\\ \dot{w}=5y_1v-\beta_m w\\ y_1=u\\ y_2=v,\end{cases}\quad\text{and}\quad(\mathrm{R}):\begin{cases}\dot{\hat{u}}=-\sigma y_1+\sigma\hat{v}\\ \dot{\hat{v}}=-20\hat{u}\hat{w}+r\hat{u}-\hat{v}\\ \dot{\hat{w}}=5\hat{u}\hat{v}-\beta_0\hat{w}\\ y_2=\hat{v},\end{cases}$$

where parameter β_m in (T) modulates the binary signal $m(t)$ as mentioned previously. The encryption algorithm $e(z,k)$ is the n-shift cipher algorithm given as

$$e(z,k)=\underbrace{f_1(\ldots(f_1}_{n}(z,\underbrace{k),k),\ldots,k)}_{n}$$

and $f_1(z,k)$ given as

$$f_1(z,k)=\begin{cases}(z+k)+2h, & -2h\le(z+k)\le-h\\ (z+k), & h\le(z+k)\le h\\ (z+k)-2h, & 2h\le(z+k)\le 2h.\end{cases}$$

where h is the encryption parameter. This means that that $-h+\beta\le\beta_m\le h+\beta$ and we have generated infinite levels of

parameters between $-h+\beta$ to $h+\beta$ using the keystream k. The parameter h is chosen in such a way that β_m is always within the range where (T) is chaotic. In (R) the parameter β_0 is set as $\beta + e(0, \hat{k})$.

The keystream k and $\hat{k}$ in (T) and (R) are generated using the Chua's system defined as

$$(\mathrm{A}):\begin{cases}\dot{p}=\alpha(q-p-\varphi(y_2))\\ \dot{q}=y_2-q-s\\ \dot{s}=-\delta q-\gamma s\\ k=d_0 p,\end{cases} \quad \text{and} \quad (\mathrm{B}):\begin{cases}\dot{\hat{p}}=\alpha(\hat{q}-\hat{p}-\varphi(\hat{y}_2))\\ \dot{\hat{q}}=\hat{y}_2-\hat{q}-\hat{s}\\ \dot{\hat{s}}=-\delta\hat{q}-\gamma\hat{s}\\ \hat{k}=d_0\hat{p}.\end{cases}$$

where d_0 is a scaling factor such that k and $\hat{k}$ lies within the interval [$-h$, h]. Note that here the signal y_2 and $\hat{y}_2$ is injected in the nonlinearity of the Chua's system. It means that the systems (A) and (B) are driven by y_2 and $\hat{y}_2$ respectively such that they synchronize with each other forming an indirect coupling.

The simulation of the proposed system is performed using Matlab/Simulink for the transmission of randomly generated digital bits. The different values used for systems (T), (R), (A) and (B) are taken as σ = 16, r = 45.6, β = 4.2, ρ = 0.1, h = 0.2, α = 10, δ = 14.87, γ = 0, d_0 = 0.05 and n for cipher shift algorithm is taken as 30.

Figure 2 shows the performance of the modified CSK method in successfully extracting the transmitted random bits. It can be seen that the random bits are successfully recovered at the receiver part using the proposed method exploiting the synchronization/desynchronization.

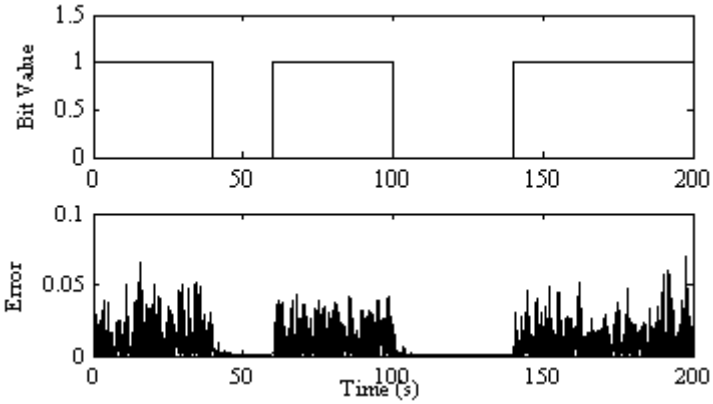

Figure 2. Transmission of random bits by CSK method using encryption and extraction.

4. Security Analysis

In this section security analysis of the proposed method using the most common decryption attack will be done. Not all of the attack methods are possible to be taken into consideration. However, Return Map (RM) being the common and the most powerful method for attacking CSK is used in this paper. RM sees the extraction of bits as a classification problem. In fact, extraction of either 0 or 1 in the transmitted signal is a classification problem, which is how digital equalization is also performed in digital communication. Other pattern classification tools can also be studied; however, if there is no pattern to classify for a method (RM in this case), it will generally mean that it will be valid for the remaining tools.

If x_i and X_i are the i-th minima and maxima for the transmitted signal y_1 respectively, then lets define $A_i = (X_i + x_i)/2$ and $B_i = (X_i + x_i)$. The plot of the B_i with respect to A_i is called RM of the signal y_1 [17].

The Figure 3 clearly illustrates the shortcoming of the classical CSK method where distinct two branches are seen when switched between only two parameters. Variation of CSK method was proposed as in [18] where authors have tried to confuse the intruders by including some switching parameters. However, there are branches in RM if the RM is zoomed in as shown in [19]. Methods like [4] has also been proposed but broken easily later [16]. As we shall show, the method proposed here, in this paper, can be employed to make the CSK method secure. The use of the keystream generated by indirect coupling synchronization at Tx and Rx will generate the parameter β_m of different values, in fact infinite possibilities within a range. The keystream generated is not part of the transmitted signal. Therefore, there is no way that the intruders will be able to generate it from only the knowledge of the transmitted carrier signal only. Without the knowledge of the keystream, it will be impossible for the intruders to find the change in the parameter $\tilde{\beta}_m$ in the receiver to perform synchronization/desynchronization for extracting the bits.

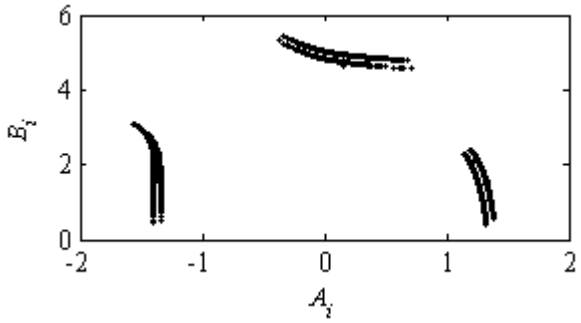

Figure 3. RM for traditional CSK scheme when β switched in two values.

Figure 4 shows the return map generated using the proposed method. It can clearly be seen that RM of the transmitted signal does not change according

to the bit values being sent. This, therefore, will remove the possibility of seeing extraction of the bits as a classification problem.Consequently, by implementing the proposed methods a secure communication can be realized. For comparison, the RM of the transmitted signal is plotted when CSK is not implemented, i.e. when the transmitted bits do not modulate the parameter of the transmitter. It can be seen in Figure 5 that the RM is similar as in Figure 4 concluding that the proposed method does not necessarily change the return map of the transmitted carrier chaotic signal.

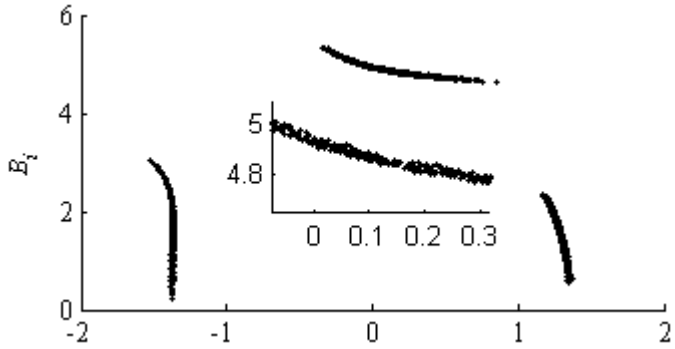

Figure 4. RM of the transmitted carrier signal using the proposed method.

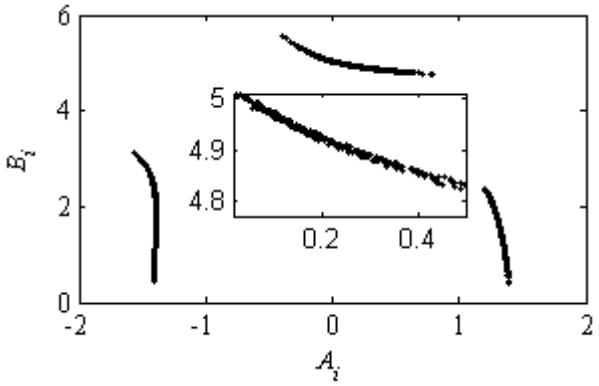

Figure 5: RM of the transmitted carrier signal when CSK is not implemented.

5. Conclusions

In this paper, the modified CSK method based on indirect coupled synchronization is proposed. The method is based on the use of an encryption algorithm whereby a chaotic keystreamb is generated using indirect coupled synchronization in the transmitter and receiver. The simulation showed that the method is able to extract the bit successfully at the receiver. Return map based attack is performed on the proposed method proving that the proposed method is secure. In fact, other pattern classification algorithm like ANN will also not be the suitable attack method because there is no pattern in the

transmitted signal as depicted by the return map. The brute force attack will also not be an effective attack because of the large key space to choose from. Switch detection will not be an effective either because of the infinite levels generated by the encryption algorithm. Simulation confirms the effectiveness of the proposed method with regards to return map attacks.

References

[1] T. Yang, "A survey of chaotic secure communication systems," *International Journal of Computational Cognition,* vol. 2, pp. 81-130, 2004.

[2] T. Yang, L. B. Yang, and C. M. Yang, "Cryptanalyzing chaotic secure communication using return maps," *Physics Letters A,* vol. 245, pp. 495-510, 1998.

[3] T. Yang, L. B. Yang, and C. M. Yang, "Application of neural networks to unmasking chaotic secure communication," *Physica D,* vol. 124, pp. 248-257, 1998.

[4] S. Bu and B.-H. Wang, "Improving the security of chaotic encryption by using a simple modulating method," *Chaos Solitons & Fractals,* vol. 19, pp. 919-924, 2004.

[5] X. Wu, H. Hu, and B. Zhang, "Analyzing and improving a chaotic encryption method," *Chaos Solitons & Fractals,* vol. 22, pp. 367-373, 2004.

[6] S. Li, G. Alvarez, and G. Chen, "Breaking a choas-based secure scheme designed by an improved modulation method," *Chaos, Solitons and Fractals,* vol. 25, pp. 109-120, 2005.

[7] C. Y. Chee, D. Xu, and S. R. Bishop, "A zero-crossing approach to uncover the mask by chaotic encryption with periodic modulation," *Chaos Solitons & Fractals,* vol. 21, pp. 1129-1134, 2004.

[8] Z. Li and D. Xu, "A secure communication scheme using projective chaos synchronization," *Chaos, Solitons & Fractals,* vol. 22, pp. 477-481, 2004.

[9] J. Y. Chen, K. W. Wong, L. M. Cheng, and J. W. Shuai, "A secure communciation scheme based on the phase synchronization of chaotic systems," *Chaos,* vol. 13, pp. 508-514, 2003.

[10] G. Alvarez, S. Li, F. Montoya, M. Romera, and G. Pastor, "Breaking projective chaos synchronization secure communication using filtering and generalized synchronization," *Chaos Solitons & Fractals,* vol. 24, pp. 775-883, 2005.

[11] G. Alvarez, F. Montoya, G. Pastor, and M. Romera, "Breaking a secure communication scheme based on the phase synchronization of chaotic systems," *Chaos,* vol. 14, pp. 274-278, 2004.

[12] K. M. Short and A. T. Parker, "Unmasking a hyperchaotic communication scheme," *Physical Review E,* vol. 58, pp. 1159-1162, 1998.

[13] C. Zhou and C. H. Lai, "Extracting messages masked by chaotic signals of time-delay systems," *Physical Review E,* vol. 60, pp. 320-323, 1999.

[14] R. Kharel, K. Busawon, and Z. Ghassemlooy, "Indirect coupled oscillators for keystream generation in secure chaotic communication," in *Proceedings of the 48th IEEE conference on Decision and Control and 28th Chinese Control Conference 2009*, 2009.

[15] P. Palaniyandi and M. Lakshmanan, "Secure digital signal transmission by multistep parameter modulation and alternative driving of transmitter variables," *International Journal of Bifurcation and Chaos,* vol. 11, pp. 2031–2036, 2001.

[16] S. Li, G. Chen, and G. Alvarez, "Return-Map Cryptanalysis Revisited," *International Journal of Bifurcation and Chaos,* vol. 16, pp. 1557-1568, 2006.

[17]G. Perez and H. A. Cerdeira, "Extracting messages masked by chaos," *Phys. Rev. Lett.,* vol. 74, pp. 1970-1973,, 1995.

[18]D. Xu and C. Y. Chee, "Chaotic encryption with transient dynamics induced by pseudorandom switching keys," *International Journal of Bifurcation and Chaos,* vol. 14, pp. 3625–3631, 2004.

[19]D. Materassi and M. Basso, "Time Scaling of Chaotic Systems: Application to Secure Communications," *International Journal of Bifurcation and Chaos,* vol. 18, pp. 567-575, 2008.